政府の情報収集はどこまで進んでいるのか——NOTICEによる侵入調査とは

- 2025/11/25
- JCA-NETセミナー
- としまる
- toshi@jca.apc.org

本日のテーマ

- 　高市政権のスパイ関連法制の取り組みを視野に入れて、19日に続いて、政府によるサイバースパイの問題を検討します。今回は、2019年から日本政府が実施しているNOTCEと呼ばれるハッキング調査の問題をとりあげます。
- 　NOTICEとは、官民が連携して、ルーターなどのIoT機器(※)にIDとパスワードを入力して、アクセス可能かどうかなどを調査するもので、プロバイダーにも協力を求めて実施されてきたものです。サイバー攻撃への対処などを理由にしていますが、政府機関が個人も含め民間が管理している通信機器に対して侵入が可能な手段をとることは、通信の秘密の侵害など様々な問題があります。このNOTICEについては、2019年の導入当時に反対運動がありました。
- 　しかし、高市政権によるスパイ関連法制への動きのなかで、NOTICEが政府による私たちの通信に対する侵入調査の悪用、つまり私たちへのスパイ活動となりうるものへと変質するおそれもあります。この点を踏まえてNOTICEとは何なのか、NOTICEと私たちの通信の秘密・プライバシーの権利との関連、そして政府によるスパイ活動に対する私たちの対抗措置を考えます。

※ 車や家電、産業用設備などでインターネットとの通信機能を備えているもの。

本日のテーマ

- NOTICEの意図を総務省のサイトなどで紹介
- NOTICEとは何なのか、民間との連携はどうなっているのか
- IoTを標的にしたサイバー攻撃とは
- 2024年法改正後の侵入調査の拡大
- 不正アクセス禁止法との関係
- 日本政府がサイバースパイ・サイバー攻撃の主体になるとき、NOTICEは転用可能か
- 私たちのできることとは



POINT

ウェブカメラやルータ、スマート家電など、家庭の中にも様々なIoT機器が増え、生活を便利にしています。一方で、セキュリティ対策が十分でないと踏み台となってサイバー攻撃に悪用されたり情報を盗まれたりするおそれがあります。こうした危険を防ぐため、令和元年（2019年）からサイバー攻撃に悪用されるおそれのある機器の利用者に注意喚起をする「NOTICE」という取組が行われています。

インターネットに接続される機器の数は年々増加しており、2020年には家電、防犯機器、自動車、医療機器、事務機器、産業機器など、200億を超える様々な「モノ」がつながる「モノのインターネット（IoT）」が形成されると言われています。



これらの「モノ」が所有する情報がネットワークを介して収集・分析・フィードバックされ、様々な形で活用されることが見込まれています。そのようなIoT機器は、インターネットを含む様々なネットワークと接続すること、プライバシーに関わる機微な情報を外部とやり取りすること、クラウドを活用すること等を前提とし、適切なセキュリティ対策が行われていることが必須となります。

NOTICEへの疑問

- IoTを悪用したサイバー攻撃や情報窃取に対して、果たして政府が取り組む「NOTICE」には問題がないのだろうか？
- 政府広報は、サイバー攻撃の注意喚起として「NOTICE」をしきりに宣伝しているが...
- 高市政権のスパイ機関創設の動きや、通信情報の広範にわたる収集を制度化しようとしている今、NOTICEの役割も変質しかねないところにきているといえないか。

左上：政府広報「ウェブカメラやルータが乗っ取られる？IoT機器のセキュリティ対策は万全ですか？」
https://www.gov-online.go.jp/article/202005/entry-9538.html
左：情報処理推進機構(IPA)「IoTのセキュリティ」
https://www.ipa.go.jp/security/iot/about.html

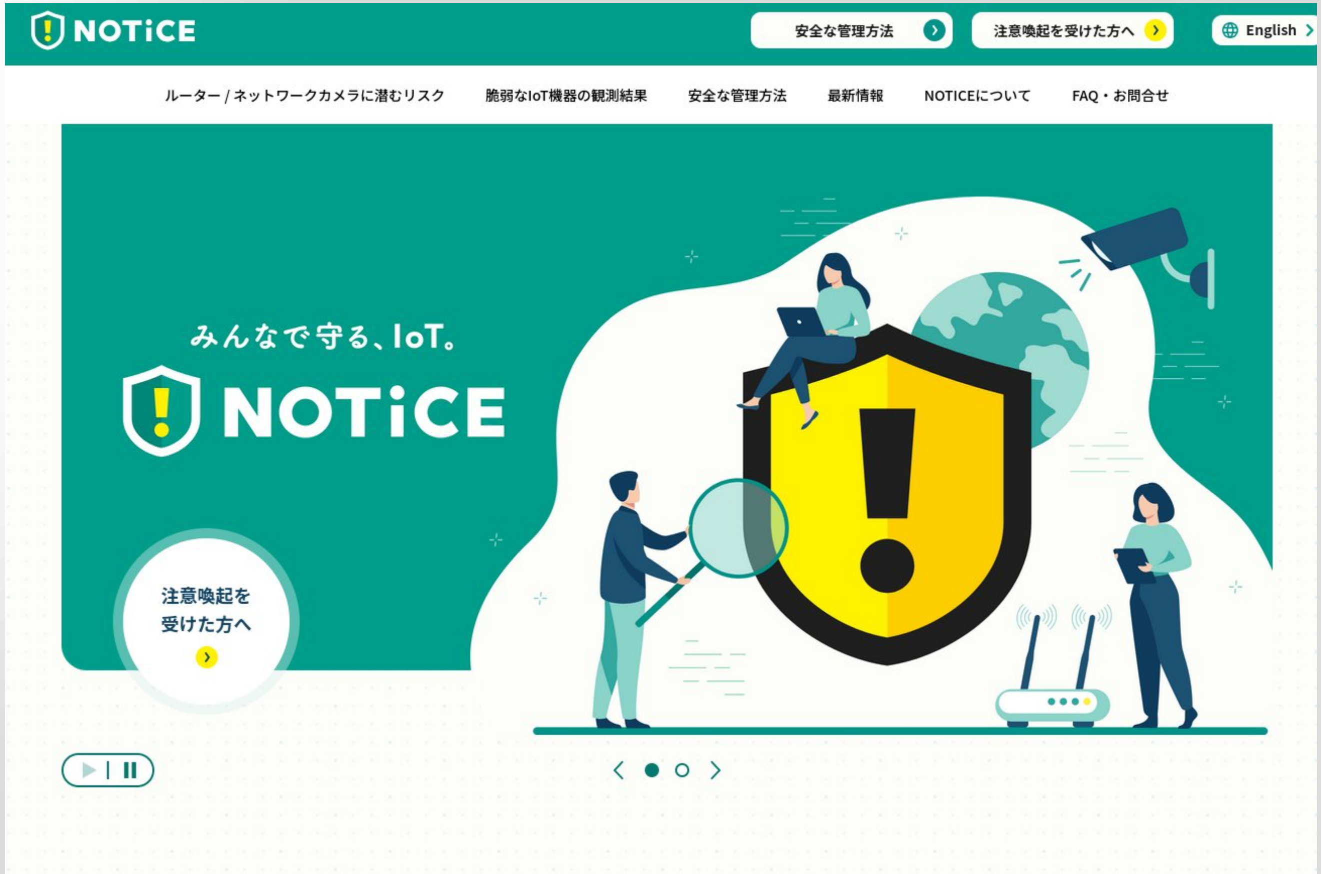
NOTICEとは
総務省のサイトから

- 総務省・国立研究開発法人情報通信研究機構（NICT）・一般社団法人ICT-ISACおよびインターネットサービスプロバイダ（ISP）・IoT機器メーカー・SIer(※)などが連携し、**IoT機器のセキュリティ対策向上を推進する**ことにより、**サイバー攻撃の発生や、その被害を未然に防ぐためのプロジェクト**
- IoT機器の安全な管理方法の広報や、危険性があるIoT機器の管理者・利用者への注意喚起を行う。
- 開始：2019年2月20日
- プロジェクト運営組織

総務省、国立研究開発法人情報通信研究機構（NICT）、一般社団法人ICT-ISAC

- 関連プロジェクト NICTER(Network Incident analysis Center for Tactical Emergency Response の略)

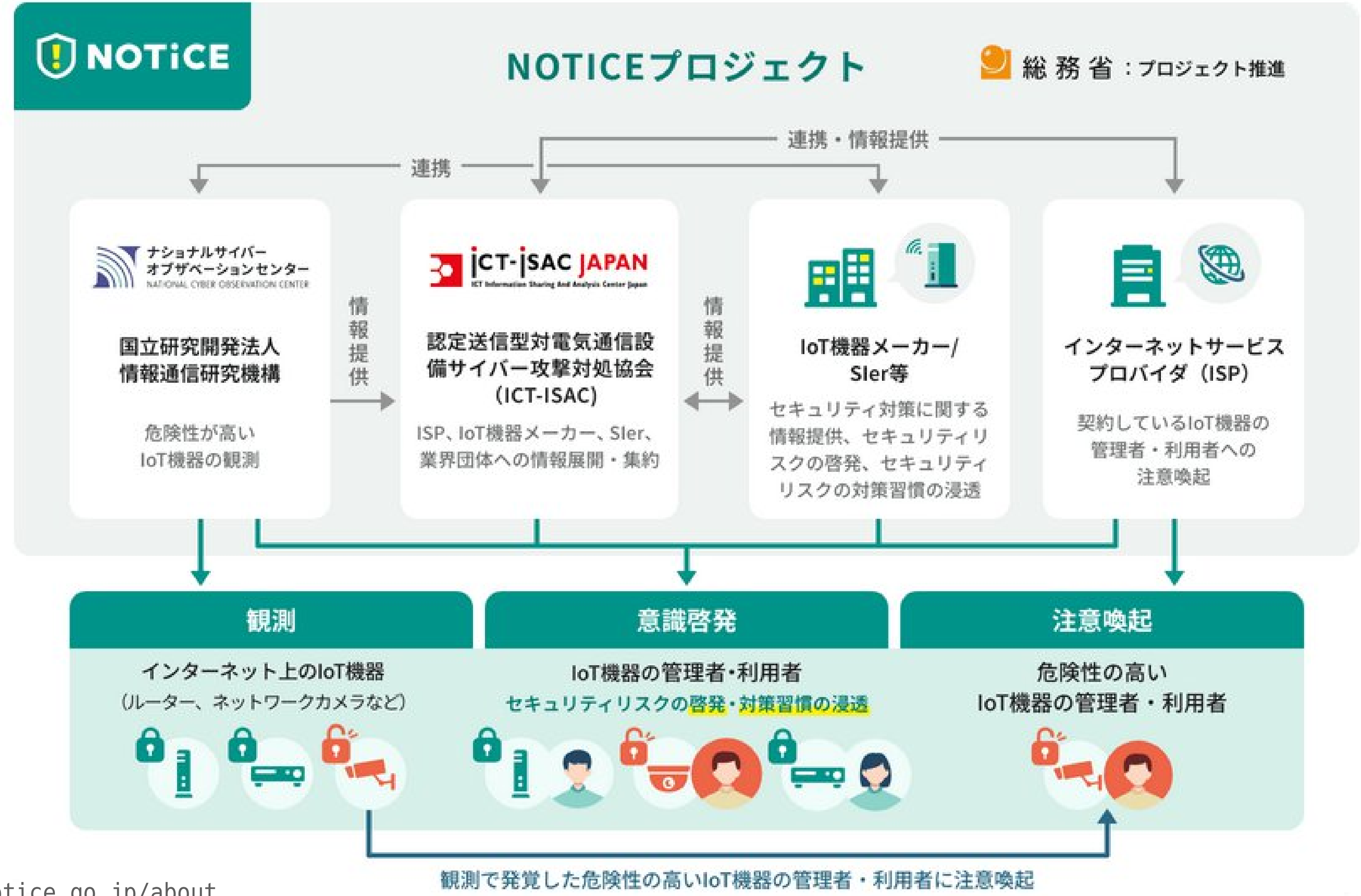
※2 SIer エスアイアー 「システム開発の、すべての工程を請け負う受託開発企業」を指す



https://notice.go.jp/

このプロジェクトは当初2022年のオリンピック・パラリンピック対策を名目に導入され、後に目的が拡大した。

NOTICEの組織紹介



ps://notice.go.jp/about

- 総務省（サイバーセキュリティ統括官室）
https://www.soumu.go.jp/main_sosiki/cybersecurity/
- 国立研究開発法人情報通信研究機構（NICT）｜ナショナルサイバーオブザベーションセンター（NCOC）
https://nco.nict.go.jp/
- 一般社団法人ICT-ISAC
https://www.ict-isac.jp/

SIer(エスアイアー)とは、「システム開発の、すべての工程を請け負う受託開発企業」のこと

- クライアントが抱える課題解決へのコンサルティング
- システムの企画立案
- システムの設計、開発
- システム導入に必要なハードウェア、ソフトウェアの選定
- システム導入に必要なインフラの構築
- システムの導入サポート
- システム運用開始後の運用保守⬚⬚⬚⬚など

https://notice.go.jp/about

参加組織

インターネットサービスプロバイダ（ISP）

- 株式会社アイ・キャン
- 株式会社秋田ケーブルテレビ
- 株式会社アクティブワークス
- 旭川ケーブルテレビ株式会社
- 株式会社朝日ネット
- 株式会社アピオン
- 株式会社アミックスコム
- アルテリア・ネットワークス株式会社
- 諫早ケーブルメディア株式会社
- イッツ・コミュニケーションズ株式会社
- 射水ケーブルネットワーク株式会社
- 株式会社インターネットイニシアティブ
- 株式会社インターネット尾張
- 株式会社インフォメーション・ネットワーク・コミュニティ
- 株式会社エコーシティー・駒ヶ岳
- 株式会社エスエーシー
- 株式会社エスイーシー
- 株式会社STNet
- 株式会社エヌ・シィ・ティ
- 株式会社エヌ・ティ・ティエムイー
- 株式会社NTTドコモ
- NTTドコモビジネス株式会社
- NTTPC コミュニケーションズ株式会社
- 株式会社エネコム
- 株式会社愛媛CATV
- 株式会社大塚商会
- 沖縄セルラー電話株式会社
- 株式会社オプテージ
- 株式会社ギガプライズ
- 株式会社キャッチネットワーク
- 株式会社QTnet
- 近鉄ケーブルネットワーク株式会社
- グリーンシティコム株式会社
- KDDI株式会社
- 株式会社KCN京都
- 株式会社KCNなんたん
- ケーブルテレビ株式会社
- 株式会社ケーブルテレビ可児
- 株式会社ケーブルテレビ品川
- 株式会社ケーブルテレビ富山
- 株式会社ケーブルネット鈴鹿
- 株式会社ケーブルワン
- 株式会社広域高速ネット二九六
- 山陰ケーブルビジョン株式会社
- GMOインターネット株式会社
- シーシーエヌ株式会社
- CTBメディア株式会社
- 株式会社シー・ティー・ワイ
- JCOM株式会社およびグループ会社10社（計11社）
- 株式会社JPIX
- 上越ケーブルビジョン株式会社
- スターキャット株式会社
- 株式会社ZTV
- ソニーネットワークコミュニケーションズ株式会社
- ソフトバンク株式会社
- 知多メディアスネットワーク株式会社
- 中部テレコミュニケーション株式会社
- 銚子インターネット株式会社
- 株式会社つなぐネットコミュニケーションズ
- 株式会社テレビ岸和田
- 株式会社テレビ九州
- 株式会社TOKAIケーブルネットワーク
- 株式会社TOKAIコミュニケーションズ
- 株式会社トークネット
- となみ衛星通信テレビ株式会社
- 株式会社trunk
- 株式会社ドリーム・トレイン・インターネット
- ニフティ株式会社
- 日本・アルカディア・ネットワーク株式会社
- 株式会社ニューメディア
- 株式会社NEXT
- 株式会社ネットフォレスト
- 株式会社ハイネット
- ビッグローブ株式会社
- ひまわりネットワーク株式会社
- 株式会社ファイバーゲート
- 株式会社福岡ソフトウェアセンター
- 富士通株式会社
- フリービット株式会社
- 株式会社ブイ・アール・テクノセンター
- 株式会社ベイ・コミュニケーションズ
- 天糸瓜ネット合同会社
- 株式会社ベッコアメ・インターネット
- 株式会社ミライコミュニケーションネットワーク
- 横浜ケーブルビジョン株式会社
- 株式会社嶺南ケーブルネットワーク

参加組織

IoT機器メーカー

株式会社アイ・オー・データ機器

i-PRO株式会社

株式会社アットマークテクノ

NECプラットフォームズ株式会社

エレコム株式会社

サン電子株式会社

株式会社Jシステム

株式会社バッファロー

ヤマハ株式会社

SIer

株式会社大塚商会

株式会社マクニカ

団体

（一社）デジタルライフ推進協会

（公社）日本防犯設備協会

https://notice.go.jp/about

何をやっている？

NOTICEの活動内容

近年、ルーターやネットワークカメラなどIoT機器を悪用したサイバー攻撃が深刻化しています。セキュリティ対策が十分に行われていないIoT機器は、マルウェアに感染し、サイバー攻撃に加担してしまう危険性があります。特に、管理機能に適切なアクセス制限を設定していない、推測しやすいパスワードを用いている、ファームウェアのアップデートを行っていないなどの場合に、サイバー攻撃に悪用される可能性が高まります。

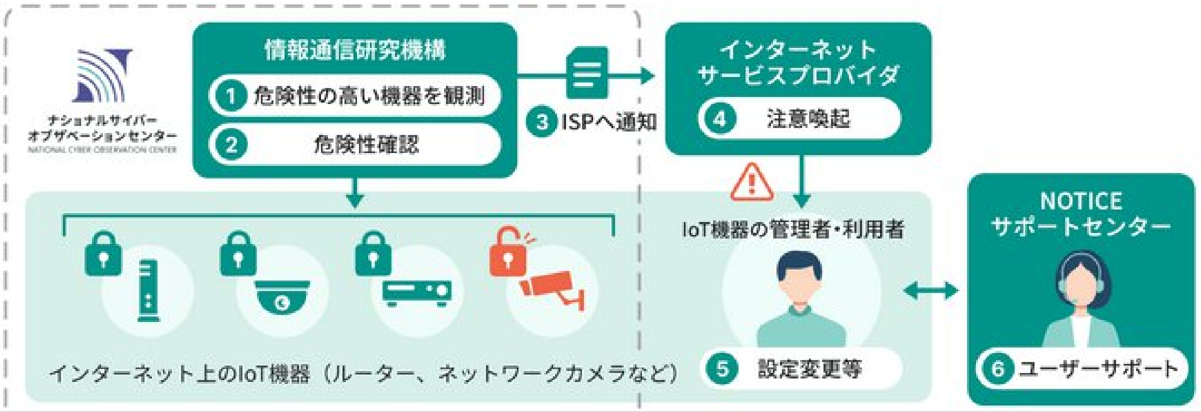
NOTICEはサイバー攻撃の予防や、被害の最小化を目的として以下の3つの活動に取り組んでいます。

- IoT機器のセキュリティリスクの啓発と対策習慣の浸透
- IoT機器のセキュリティ対策に関する充実した情報提供
- 危険性が高いIoT機器の観測と管理者・利用者への注意喚起

経緯
2019年から5年の時限立法で開始
2023年　法改正によって継続。同時に、調査対象を拡充

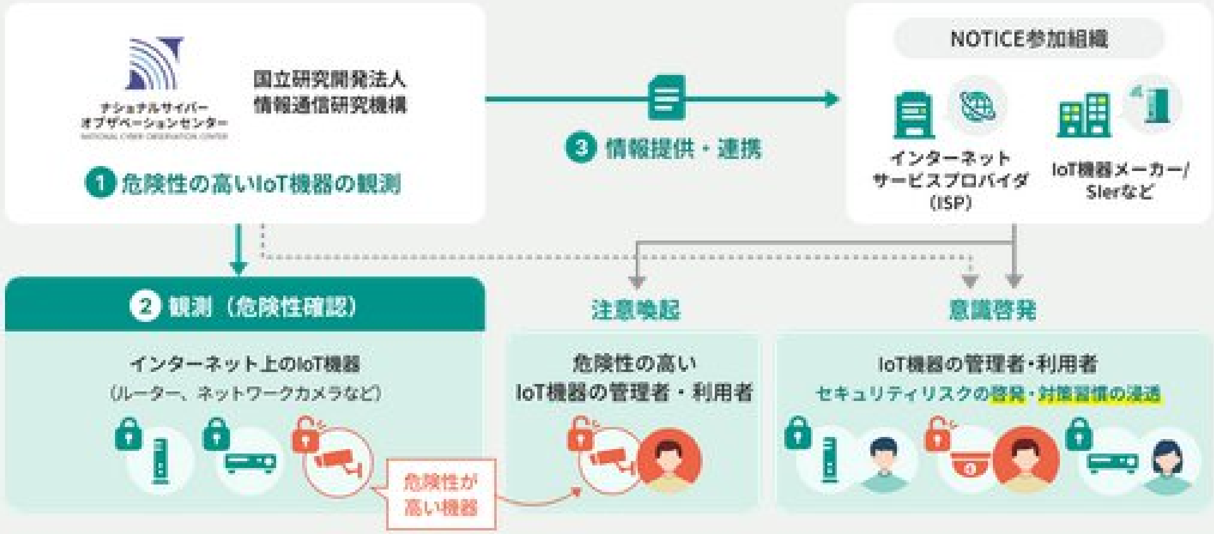
https://notice.go.jp/about

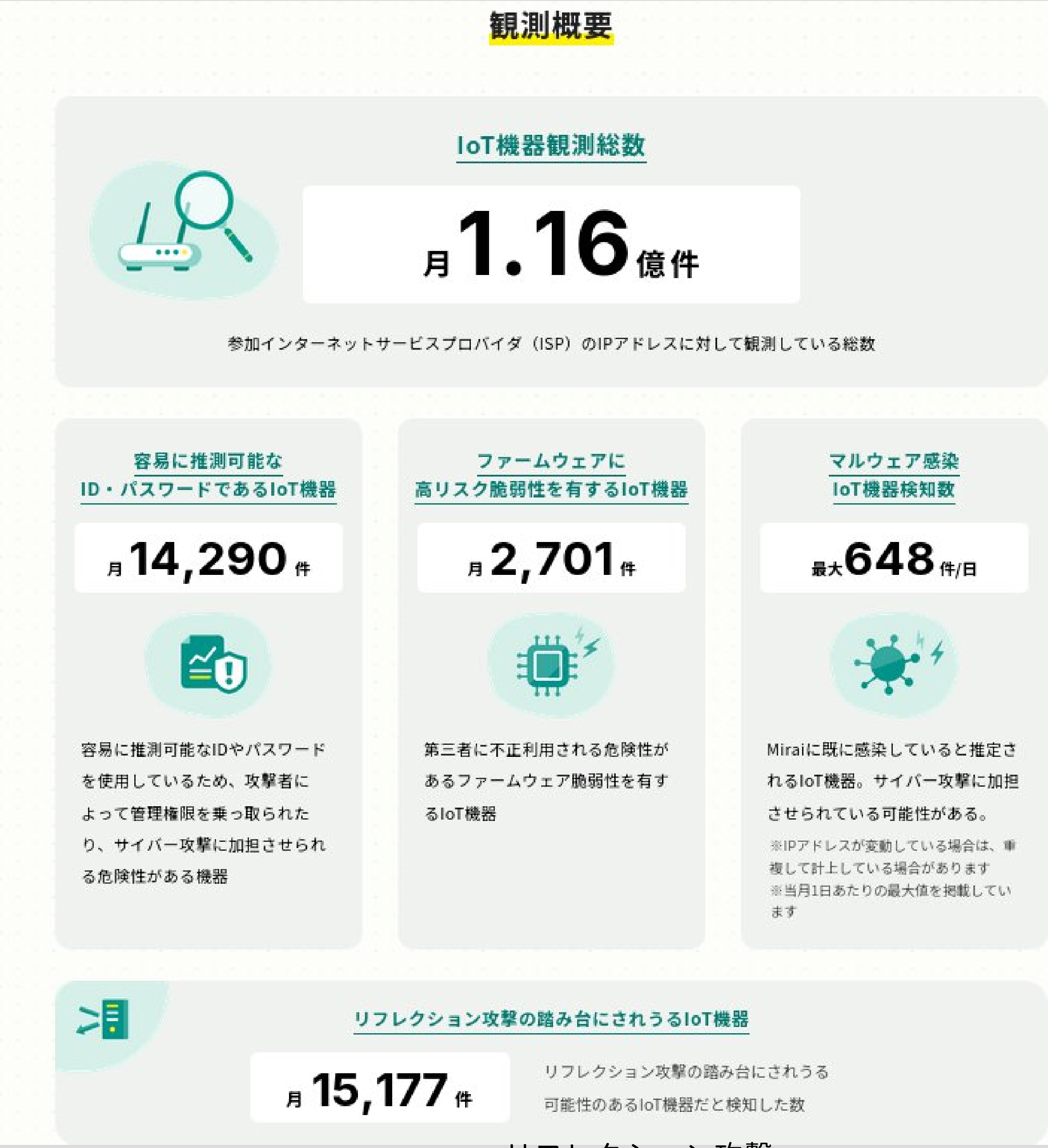
1. NOTICEに協力しているISPのネットワークに直接接続されているIoT機器を定期的に観測（パソコンやスマホは観測の対象外です）
2. 1で観測したIoT機器のうち、サイバー攻撃に悪用されている、または悪用されるおそれがあるIoT機器を、危険性が高いIoT機器として特定
3. 2で特定した危険性が高いIoT機器の、グローバルIPアドレスや脆弱性などの情報をISPに通知
4. NICTから通知を受けたISPが当該IoT機器の管理者・利用者に対して、電子メールや郵便で注意喚起を実施
5. 注意喚起を受けたIoT機器の管理者・利用者は、IoT機器の設定変更などのセキュリティ対策を行う
6. サポートが必要な方には、NOTICEサポートセンターがIoT機器設定方法などをご案内



何をやっている？

(1)NOTICEに参加しているISPのネットワークに接続　されているIoT機器を定期的に観測
(2)（1)で観測したIoT機器のうち、サイバー攻撃に悪用されている、または悪用される脆弱性のあるIoT機器を、危険性が高いIoT機器として特定
(3)（2)で特定した危険性が高いIoT機器のグローバルIPアドレスや脆弱性などの情報をISPに通知





https://notice.go.jp/observation

https://notice.go.jp/status

リフレクション攻撃
https://knowledge.sakura.ad.jp/6348/

(まとめ)NOTICEとは

政府

↓

論点1

ルーター、ネットワークカメラなどのIoT機器に対して侵入できるかチェック

↓

侵入できれば、プロバイダーなどに通知

→

IoT機器のユーザー

↓

論点2

対処
- パスワード変更
- セキュリティアップデート
- 機器の買い替え

論点1 政府が侵入調査をすることの問題はないのか？プロバイダーが侵入調査を容認することに問題はないのか？

論点2 ユーザーは政府の侵入調査に頼らなければ、リスク・脆弱性を解決できないのか？

(攻撃事例)IoTを利用したMiraiのばあい

攻撃者

脆弱性のあるIoT機器
を探索

攻撃の指令を出す
(C&Cサーバ)

1

脆弱性のあ
るIoT機器

脆弱性のあ
るIoT機器

脆弱性のあ
るIoT機器

2

3

Mirai(マルウェア)をインストール

脆弱性のあ
るIoT機器

脆弱性のあ
るIoT機器

脆弱性のあ
るIoT機器

4

標的のシステム

攻撃は、大量のデータを
送り込むことでシステム
のダウンを狙う

Miraiは、2016年9月13日夜、米国のセキュリティジャーナリストBrian Krebs氏のWebサイトに対して行われた大規模なDDoS攻撃に使用されたとして話題になったボットネット。Miraiは主にWebカメラやルーター、デジタルビデオレコーダーなどのIoTデバイスを踏み台としてDDoS攻撃を仕掛ける。

https://atmarkit.itmedia.co.jp/ait/articles/1611/08/news028.html

2024年法改正後の侵入調査の拡大

国立研究開発法人情報通信研究機構法の一部を改正する等の法律の概要

NICTが行うサイバー攻撃に悪用されるおそれのあるIoT機器の調査について、①令和５年度末に時限を迎えるID・パスワードに脆弱性があるIoT機器の調査を、令和６年度以降も継続的に実施を可能とするとともに、②調査の対象を拡充するための規定を整備する。あわせて、特定通信・放送開発事業実施円滑化法の廃止等を行う。

１．サイバーセキュリティ関連業務の規定の整備

［国立研究開発法人情報通信研究機構法の改正］

① ID・パスワードに脆弱性があるIoT機器の調査の継続的な実施

○ NICTが令和５年度末までに限り行うこととされているID・パスワードに脆弱性があるIoT機器の調査（特定アクセス行為）を、令和６年度以降も継続的に実施できることとする。

② 調査対象の拡充

○ NICTが行うIoT機器の調査等に係る業務について、その対象を拡充※するとともに、総務大臣が、サイバーセキュリティ戦略本部から意見を聴取した上で、NICTの中長期目標の策定等をする旨を規定する。

※ID・パスワードに脆弱性があるIoT機器に加えて、脆弱性があるファームウェア等を搭載しているIoT機器、既にマルウェアに感染しているIoT機器を新たに対象とする。

２．信用基金の清算及び特定通信・放送開発事業実施円滑化法の廃止等

［・国立研究開発法人情報通信研究機構法の改正
・特定通信・放送開発事業実施円滑化法（NICTの業務特例を規定）の廃止］

○ NICTの信用基金を清算し、これに伴い、NICTの関連業務及び当該基金に係る業務を規定する特定通信・放送開発事業実施円滑化法を廃止する。

施行期日：令和６年４月１日（一部の規定を除く。）

一般にIoT侵入調査ではスマホやパソコンを含めていないとされている。

しかし、総務省は情報通信白書で「IoTで想定している接続されるモノは、接続機器の従来の代表格である**パソコンやスマートフォンだけではなく、車や家電、産業用設備など、従来通信機能を備えていなかった機器**が挙げられる。」と記載している。パソコンやスマホも含まれうるような曖昧な定義だ。

2024年法改正で、「**ファームウェア等を搭載しているIoT**」**を追加の調査対象**にした。**パソコンやスマホにはファームウェアが搭載されており、IoTとしても使える**ので、従来は調査対象にしていなかったこれら機器も対象に含める意図があるかもしれない。スマホ、パソコンと明記すると大騒動になるので、巧妙に隠したともいえる？

不正アクセス禁止法との関係

不正アクセス禁止法

- 不正アクセス行為の禁止等に関する法律（禁止法）は、不正アクセス行為や、**不正アクセス行為につながる識別符号の不正取得・保管行為、行為を助長する行為等を禁止する法律**です。
- **識別符号とは、情報機器やサービスにアクセスする際に使用するIDやパスワード等**のことです。行為とは、そのようなIDやパスワードによりアクセス制御機能が付されている情報機器やサービスに対して、**他人のID・パスワードを入力したり、脆弱性（ぜいじゃくせい）を突いたりなどして、本来は利用権限がないのに、不正に利用できる状態にする行為**をいいます。総務省 https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/legal/09/

⇩

国立研究開発法人情報通信研究機構（NICT）が実施計画に基づき、容易に推測されるID、パスワードを外部から入力し、サイバー攻撃に悪用されるおそれのあるIoT機器を特定することは、**NICT法において<u>特定アクセス行為</u>とされており、不正アクセス禁止法で禁止されている不正アクセス行為から除外されています。**
また、特定アクセス行為以外のポートスキャンなどの観測は、不正アクセス禁止法で禁止されている不正アクセス行為ではありません。

不正アクセス禁止法との関係

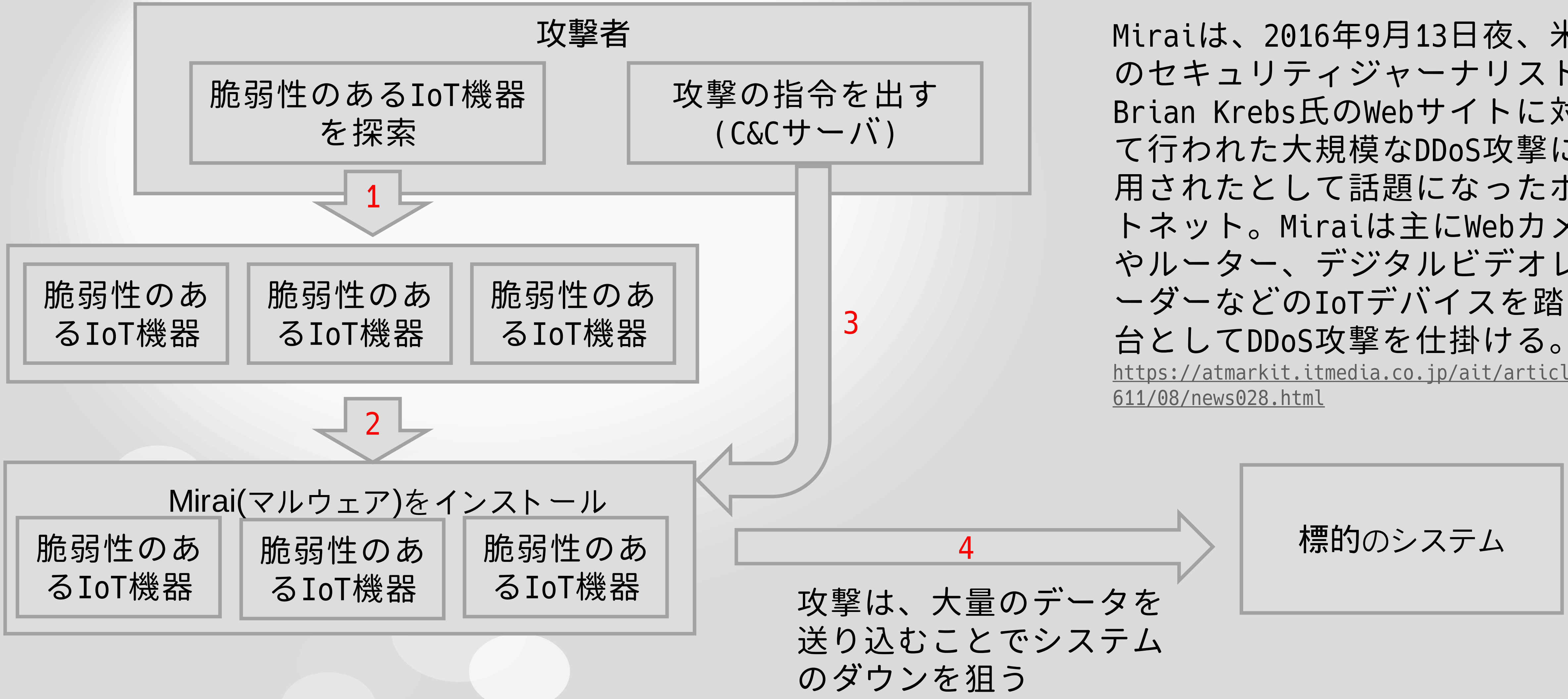
NOTICEの侵入テストは、技術的には不正アクセス禁止法で禁止されている不正アクセス行為と同じ行為。しかし、特例として、NICT法で不正アクセスとはみなさない、という法的な枠組がとられている。⇒法的例外措置が今後拡大する畏れがある？

法的規制や保護は、現在の「安心」でしかなく、将来の改悪はいくらでもありえる。

- 政府がいう「アクセス・無害化措置」や通信情報の広範囲にわたる収集が制度化された場合、NOTICEの役割も変質する可能性。
- 現在禁じられているスマホやパソコンへの侵入調への拡大。
- 国外のネットワークへの「不正アクセス」行為の可能性。
- 日本政府がNOTICEで構築してきた官民連携の枠組がそのまま日本政府によるサイバー・スパイ、サイバー・攻撃の組織的な基盤の一部に転用される可能性。
- NOTICEを主導しているNICTがNATOのサイバー軍事演習に参加していることから、今後更に軍事安全保障への関与を深めるおそれ。

サイバー領域において法の支配は万全ではない。法による規制は必要条件だが十分条件ではない(アテにならない)。
だから、自分たちでセキュリティを確保する必要があるし、このような対処は可能でもある。

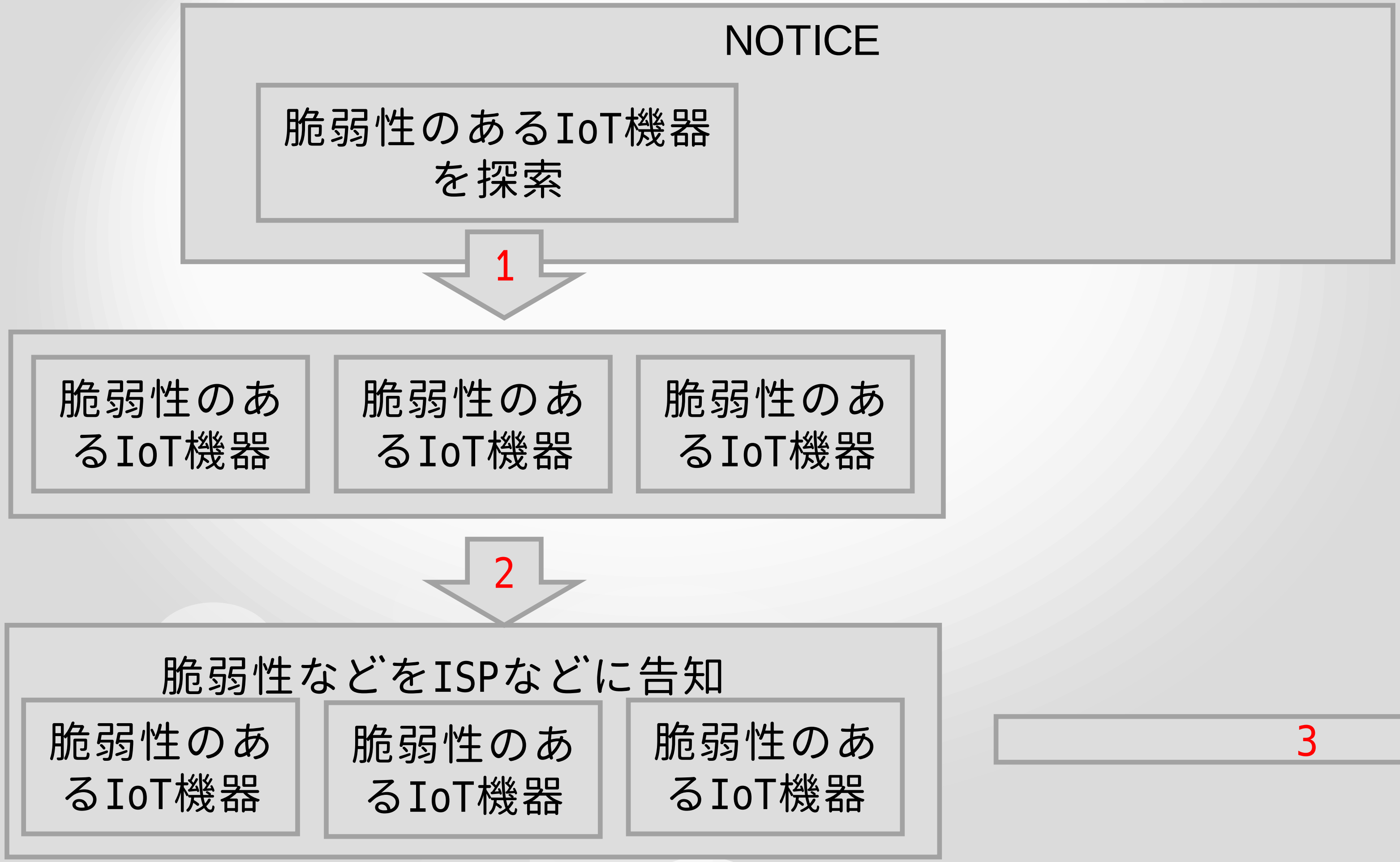
NOTICEはスパイ・攻撃の手段にも転用できる？ Miraiとの違いは？

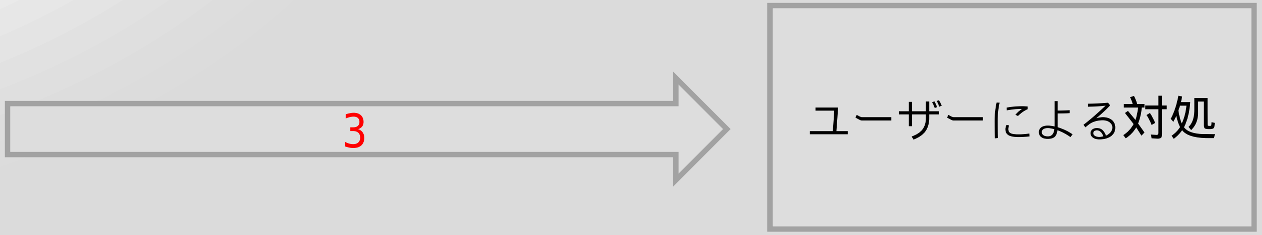


Miraiは、2016年9月13日夜、米国のセキュリティジャーナリストBrian Krebs氏のWebサイトに対して行われた大規模なDDoS攻撃に使用されたとして話題になったボットネット。Miraiは主にWebカメラやルーター、デジタルビデオレコーダーなどのIoTデバイスを踏み台としてDDoS攻撃を仕掛ける。

https://atmarkit.itmedia.co.jp/ait/articles/1611/08/news028.html

NOTICEはスパイ・攻撃の手段にも転用できる？ Miraiとの違いは？



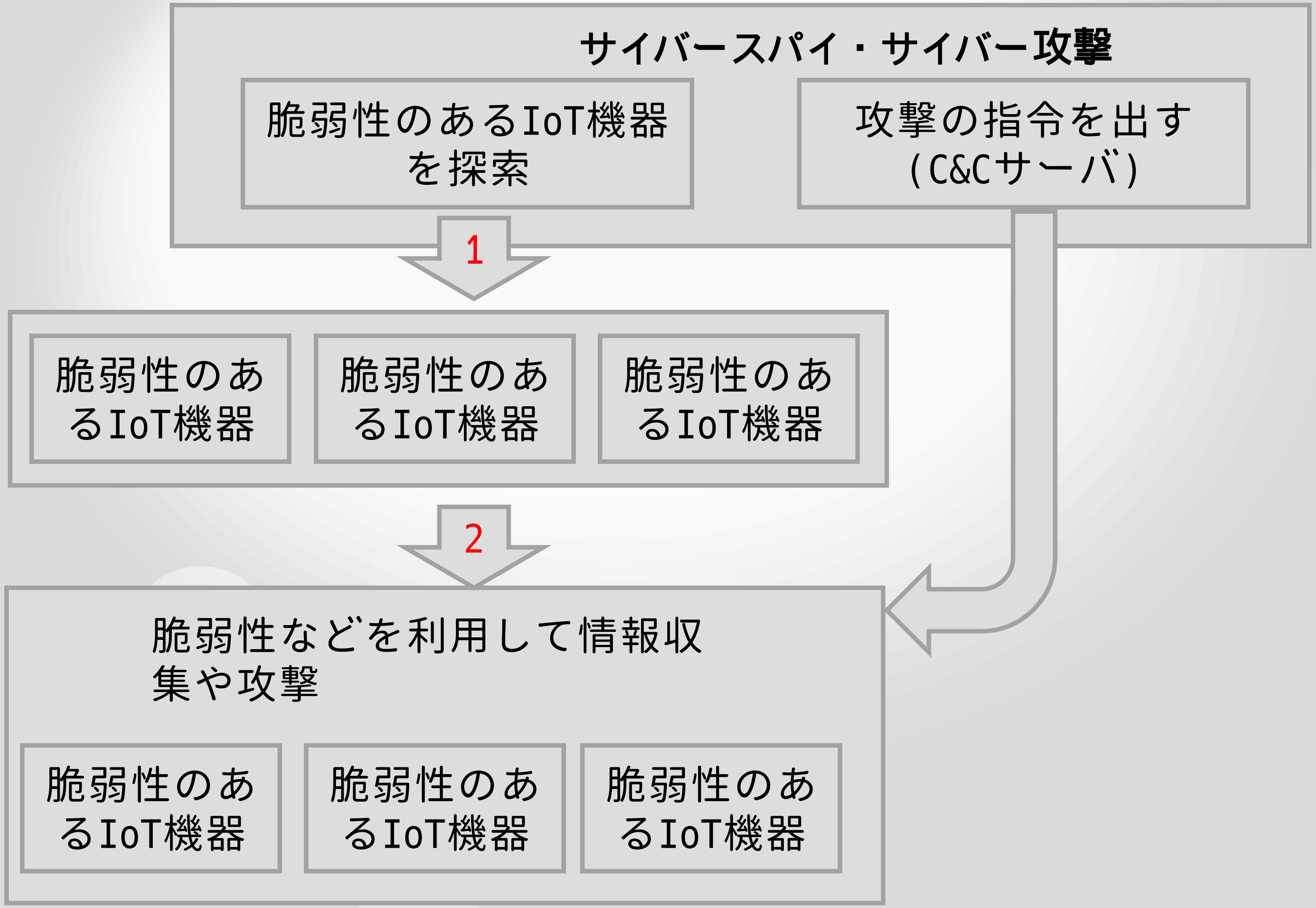


NOTICEは、Miraiのように攻撃はしないが、侵入を試み、脆弱性のある機器を探査する手法は類似している。

- NOTICEはIoTを探査することは許されているが、パソコンやスマホを探査することは法的に禁じられている。
- 脆弱性の調査のみが法的に許されている。侵入して情報を収集したりソフトウェアをインストールするなどは禁じられている。

スパイ機関の創設など法制度が変われば、同種の技術でスパイや攻撃の手段として転用可能だ。

NOTICEはスパイ・攻撃の手段にも転用できる？ Miraiとの違いは？



NOTICEのような手法を利用して、侵入を試み、脆弱性のある機器を探査する手法は通信情報を収集したりスパイウェアをインストールするなどの技術に転用できるかもしれない。

スパイ機関の創設など法制度が変われば、同種の技術でスパイや攻撃の手段として転用することが法的にも認められるかもしれない。

私たちにできることは？

2019年、IoT侵入調査開始の際に出された中止要求の共同声明

総務省、国立研究開発法人情報通信研究機構(NICT)による 「IoT機器調査」の中止を強く求めます

https://www.jca.apc.org/shiminren/%e7%b7%8f%e5%8b%99%e7%9c%81%e3%80%81%e5%9b%bd%e7%ab%8b%e7%a0%94%e7%a9%b6%e9%96%8b%e7%99%ba%e6%b3%95%e4%ba%ba%e6%83%85%e5%a0%b1%e9%80%9a%e4%bf%a1%e7%a0%94%e7%a9%b6%e6%a9%9f%e6%a7%8bnict-%e3%81%ab/

- いままで、インターネットに接続するものといえばすぐ思いだすものはパソコンであったり、スマートフォンでしたが、現在、テレビ、エアコンなど家庭家電をはじめ家庭や会社内の事務機器、監視ロボット、クルマなどがインターネットに接続するようになりました。今後この傾向は更に強まります。

- 今回の調査は政府による違法なハッキング行為であると判断し、これに強く反対し、実施の中止を求めるものです。

私たちにできることは？

2019年、IoT侵入調査開始の際に出された中止要求の共同声明

総務省、国立研究開発法人情報通信研究機構(NICT)による 「IoT機器調査」の中止を強く求めます（9団体の呼びかけ）

https://www.jca.apc.org/shiminren/%e7%b7%8f%e5%8b%99%e7%9c%81%e3%80%81%e5%9b%bd%e7%ab%8b%e7%a0%94%e7%a9%b6%e9%96%8b%e7%99%ba%e6%b3%95%e4%ba%ba%e6%83%85%e5%a0%b1%e9%80%9a%e4%bf%a1%e7%a0%94%e7%a9%b6%e6%a9%9f%e6%a7%8bnict-%e3%81%ab/

- 通信の秘密を保障する憲法２１条に違反します。
- 裁判所の令状すらなしに、政府による個人のプライバシー情報への網羅的なアクセスを許す先例
- 技術的には機器内部への侵入が可能な方法をとっている
- 用いられる技術が本当に総務省の主張通りに運用されるのかどうかも、公正な第三者による検証がなされていない
- 取得情報の安全性、政府内部での情報共有のありかたなども不透明なまま
- 今回の調査について「センサーやウェブカメラなどのIoT機器」に限定されているかの印象を与えている
- 一般市民だけでなく、報道機関、弁護士事務所、人権団体、野党、労働組合、プロバイダーなどの言論・表現の自由、通信の秘密に関わる組織にも深刻な影響が及ぶ
- 将来的には、プロバイダーが取得しているIoT利用者の個人情報を政府がより容易に、あるいは直接取得するような方向へと制度や技術が変えられるきっかけになりえる

残念なことに、当時の危惧のほとんどが現実のものになってしまった

私たちにできることは？

政府に侵入させないこと=誰であれ意図しない者のアクセスをさせない

セキュリティの基本を実践することで侵入を阻止できる

- 初期設定のパスワードを変更
  - パスワードの使い回しはしない
  - 推測されやすいパスワードは使わない
  - なるべく長いパスワードを設定する
- IoTのソフトウェア(ファームウェア)を最新のものにアップデートする
- サポートが終了したIoTは使わない
- ネットに接続する必要のないものはネットから切断する

しかし、IoTのパスワードなどの設定をチェックし、変更することは慣れないので、戸惑うかもしれない。そのときは、ぜひDigital-rightsのメーリングリストに相談してみてください。

(参考)国立研究開発法人情報通信研究機構法

特定アクセス行為　機構の端末設備又は自営電気通信設備を送信元とし、アクセス制御機能を有する特定電子計算機である電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備を送信先とする電気通信の送信を行う行為であって、当該アクセス制御機能を有する特定電子計算機である電気通信設備に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号（当該識別符号について電気通信事業法第五十二条第一項又は第七十条第一項第一号の規定により認可を受けた技術的条件において定めている基準を勘案して不正アクセス行為から防御するため必要な基準として総務省令で定める基準を満たさないものに限る。）を入力して当該電気通信設備を作動させ、当該アクセス制御機能により制限されている当該電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備の特定利用をし得る状態にさせる行為をいう。

二　通信履歴等の電磁的記録　特定アクセス行為に係る電気通信の送信元、送信先、通信日時その他の通信履歴を含む特定アクセス行為についての電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。）であって、当該特定アクセス行為に係る電気通信の送信先のアクセス制御機能を有する特定電子計算機である電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備を送信先又は送信元とする送信型対電気通信設備サイバー攻撃のおそれがあることの証拠となるものをいう。

https://laws.e-gov.go.jp/law/411AC0000000162

(参考)不正アクセス禁止法の条文

第二条
この法律において「不正アクセス行為」とは、次の各号のいずれかに該当する行為をいう。
一　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。）
二　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。次号において同じ。）
三　電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為

https://laws.e-gov.go.jp/law/411AC0000000128

参考サイト

政府のNOTICEの公式サイト
https://notice.go.jp/

Wi-Fi のセキュリティとプライバシー――現状と対策(JCA-NETセミナー2025年9月資料)
https://pilot.jca.apc.org/nextcloud/index.php/s/yBH2Y4fR5ZQkcG7

プレスリリース「IoT機器のセキュリティ向上を推進する新しい「NOTICE」を開始」(2024年3月29日総務省 国立研究開発法人情報通信研究機構 一般社団法人ICT-ISAC)
https://www.nict.go.jp/press/2024/03/29-2.html

新しい NOTICE の船出－国内の IoT セキュリティの最新状況－2025/02/21 NICT サイバーセキュリティシンポジウム 2025 国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所ナショナルサイバーオブザベーションセンター (NCO)研究センター長 衛藤 将史
https://www2.nict.go.jp/csri/nict_cyber2025/Presentation%20materials_masashi-eto.pdf

より安全な IoT 環境の実現に向けて－ NOTICE 事業 5 年間の総括と今後の取り組み －2024 年 2 月 16 日 NICT サイバーセキュリティシンポジウム 2024 同上 衛藤 将史

https://www2.nict.go.jp/csri/nict_cyber2024/pdf/%E8%AC%9B%E6%BC%942_%E3%82%88%E3%82%8A%E5%AE%89%E5%85%A8%E3%81%AA%20IoT%20%E7%92%B0%E5%A2%83%E3%81%AE%E5%AE%9F%E7%8F%BE%E3%81%AB%E5%90%91%E3%81%91%E3%81%A6_NOTICE%20%E4%BA%8B%E6%A5%AD%205%20%E5%B9%B4%E9%96%93%E3%81%AE%E7%B7%8F%E6%8B%AC%E3%81%A8%E4%BB%8A%E5%BE%8C%E3%81%AE%E5%8F%96%E3%82%8A%E7%B5%84%E3%81%BF.pdf

NICTER観測レポート
https://csl.nict.go.jp/report/NICTER_report_2024.pdf

政府広報「ウェブカメラやルータが乗っ取られる？IoT機器のセキュリティ対策は万全ですか？」
https://www.gov-online.go.jp/article/202005/entry-9538.html

参考サイト

電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律（平成30年法律第24号） の施行に伴う省令の制定について（NICT法の一部改正に伴う識別符号の基準及び実施計画に関する規定整備関係） 2018年8月総務省 サイバーセキュリティ統括官室
https://www.soumu.go.jp/main_content/000579753.pdf
※ 国立研究開発法人情報通信研究機構法を改正して侵入調査を合法化した際の説明資料

国立研究開発法人情報通信研究機構法第１８条第２項に規定する特定アクセス行為等実施計画の認可について(2024)
https://www.soumu.go.jp/main_content/000936394.pdf
※侵入調査(特定アクセス行為)を実施する際に必要な認可の書類

「諮問を要しない軽微な事項について」の一部改正について（国立研究開発法人情報通信研究機構法第１８条第２項に規定する特定アクセス行為等実施計画の認可について）(2024)
https://www.soumu.go.jp/main_content/000936395.pdf
※ 特定アクセス行為等に係る設備に関する事項、識別符号の方針に基づき入力する識別符号などを諮問の要件から外した。これらを「軽微な事項」といえるか疑問。

参考サイト

令和六年総務省令第十一号
特定アクセス行為等実施計画及び識別符号の基準に関する省令
https://elaws.jp/view/506M60000008011

[解説サイト]

日立　「IoT製品を狙ったサイバー攻撃の脅威！事例と対策」
https://www.hitachi-solutions.co.jp/security/sp/column/iot/03.html

IonD0「IoT機器によるサイバー攻撃を未然に防ぐ！NOTICEプロジェクトとは（総務省＆NICT）」
https://note.com/1ondo/n/n0facc1c50b90

IoTハッキング事例3選と有効なセキュリティ対策
https://cybersecurity-info.com/column/40626/

(共同声明)総務省、国立研究開発法人情報通信研究機構(NICT)による　「IoT機器調査」の中止を強く求めます(2019年2月15日)
https://www.jca.apc.org/shiminren/%e7%b7%8f%e5%8b%99%e7%9c%81%e3%80%81%…